Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 4, April 2024

Android Graphical Password

Ms.E.Indhuja
Assistant Professor, Department of Computer Science and Engineering
Kalasalingam Academy of Research and Education
Virudhnagar, Tamil Nadu, India

M.Poorna Chandra
Department of Computer Science and Engineering
Kalasalingam Academy of Research and Education
Virudhnagar, Tamil Nadu, India

M.Prasanth
Department of Computer Science and Engineering
Kalasalingam Academy of Research and Education
Virudhnagar, Tamil Nadu, India

K.Vikranth Chowdary
Department of Computer Science and Engineering
Kalasalingam Academy of Research and Education
Virudhnagar, Tamil Nadu, India

R.Raja Sekhar
Assistant Professor,Department of Computer Science and Engineering
Kalasalingam Academy of Research and Education
Virudhnagar, Tamil Nadu, India

***Abstract*— Discretization serves as a conventional method applied in click-based graphical passwords to accommodate input variations, thereby allowing the system to accept passwords that are approximately correct. This study demonstrates, for the first time, that two prevalent discretization techniques divulge a substantial amount of password information, posing a threat to the security of graphical passwords. Exploiting this information leakage, we conducted successful dictionary attacks on Persuasive Graphic Passwords with Image Selection (PGPIS), previously considered the most secure click-based graphical password scheme resistant to such breaches. Our automated attack effectively predicted 69.2% of the passwords when Centered Discretization was employed in PGPIS, and 39.4% when Robust Discretization was used. Despite dictionaries containing only a fraction of the password space, our attack successfully compromised a significant portion of the passwords. Notably, even with a reduced dictionary size of approximately entries, our attack still achieved a 50% success rate with Centred Discretization. Furthermore, our attack methodology is applicable to prevalent implementations of other click-based graphical password systems, including Pass Points and Cued Click Points, both extensively scrutinized in academic research.**

***Keywords*: Persuasive Graphic Passwords with Image Selection (PGPIS), robust discretization, Cued Click Point (CCP) technique.**

I. INTRODUCTION

User authentication methods have evolved significantly from traditional text-based passwords to graphical alternatives, offering improved memorability and resistance against guessing attacks. With the inception of graphical passwords by Blonder in 1996, users interact with images to create or enter passwords, particularly advantageous on devices like iPads and iPhones where text input is cumbersome. The proposed project introduces an innovative approach where users submit an image as their password, which the system then segments into an array of images for storage. During login, the segmented image is displayed in a jumbled order, requiring the user to arrange the parts correctly to authenticate successfully, leveraging image segmentation based on coordinates for heightened security.

In the realm of cybersecurity, graphical passwords are gaining prominence as a visually intuitive authentication mechanism, especially on mobile platforms like Android. This study focuses on integrating Cued Click Points (CCP) and Persuasive Graphic Passwords with Image Selection (PGPIS) into Android applications to enhance both security and usability. CCP allows users to select click points from a grid overlay on an image, while PGPIS guides users in choosing diverse and secure click points, reducing the risk of easily guessable passwords. Through usability testing and security evaluations, this research aims to explore the effectiveness of graphical password systems in mitigating authentication risks on mobile platforms, offering insights into user experience and security implications for future development and implementation.

II. LITERATURE SURVEY

Sonia Chiasson, P.C. van Oorschot, and Robert Biddle, Evaluating Cued Click Points: A Study of Graphical Password Strategy, Proceedings of the 2020 IEEE Symposium on Security and Privacy, Authors: Year: 2020

Methodology: This paper presents an examination of Cued Click Points (CCP) as a graphical password strategy, encompassing design, implementation, and evaluation. The methodology includes user studies to gauge CCP's usability and security in comparison to traditional alphanumeric passwords.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 4, April 2024

Limitations: The study's scope of users might be restricted, and it may not have encompassed all potential attack vectors against CCP.
Sonia Chiasson, Elizabeth Stobert, and P.C. van Oorschot, Persuasive Cued Click-Points: Enhancing Knowledge-Based Authentication, ACM Transactions on Information and System Security (TISSEC), 2021

Methodology: This paper introduces Persuasive Cued Click-Points (PCCP) and evaluates its impact on the security of graphical passwords. Methodologically, user studies and performance evaluations were conducted to assess how persuasive cues influence users' selection of secure click points.

Limitations: The study's generalizability to diverse user demographics or real-world usage scenarios might be limited.
Julie Thorpe and Mary Ellen Zurko, Exploring Graphical

Passwords: Tolerance and Image Choice, Proceedings of the Symposium on Usable Privacy and Security (SOUPS), 2020

Methodology: This paper investigates the influence of tolerance and image selection on the usability and security of graphical password systems. The methodology comprises user studies examining how tolerance settings and image choices affect users' password creation and authentication experiences.

Limitations: Findings might be influenced by the specific images and tolerance parameters chosen for evaluation, potentially affecting generalizability.
Yue Liu, Paul Dunphy, and M. Angela Sasse, Framework for Assessing Graphical Password Schemes, International Journal of Computer Applications, 2021

Methodology: This paper proposes a systematic framework for evaluating graphical password schemes, considering security and usability. The methodology involves developing evaluation metrics and guidelines for conducting user studies and security analyses.

Limitations: Further validation and refinement may be necessary to assess the framework's applicability across diverse contexts.
Pradeep Kumar Tiwari and Praveen Ranjan Srivastava, Survey of Graphical Password Authentication with Persuasive Cues, International Journal of Network Security & Its Applications (IJNSA), 2020

Methodology: This paper conducts a survey of graphical password authentication techniques, emphasizing persuasive cues. The methodology entails reviewing existing literature and synthesizing findings to identify trends, challenges, and opportunities.

Limitations: The survey's coverage of persuasive graphical password schemes might be affected by the availability and accessibility of relevant research papers, potentially introducing biases.
Sivakumar Viswanathan and M. Hemalatha, Comprehensive Survey of Graphical Password Techniques, International Journal of Computer Applications, 2020

Methodology: This paper provides a thorough survey of graphical password techniques, including CCP. Methodologically, it reviews existing literature, categorizes graphical password schemes, and analyzes their strengths, weaknesses, and usability aspects.

Limitations: The survey's coverage and analysis of graphical password techniques might be influenced by the authors' expertise and familiarity with the field, potentially leading to subjective judgments or oversights.

III. METHODOLOGY

We've proposed an alternative technique resistant to shoulder surfing. This method involves users selecting a series of pictures as pass-objects, each with multiple variants, each variant assigned a unique code. During authentication, users are presented with various scenes containing pass-objects (each represented by a randomly chosen variant) and decoy-objects. Users must input a string consisting of the unique codes corresponding to the pass-object variants in the scene, along with a code indicating the relative location of the pass-objects in reference to a pair of eyes. This approach makes it challenging to crack the password, even if the authentication process is recorded, as there are no mouse clicks revealing pass-object information. However, users still need to memorize alphanumeric codes for each pass-object variant, which can be cumbersome. To address this, we've extended the method to allow users to assign their own codes to pass-object variants. Nonetheless, this still requires users to memorize multiple text strings, suffering from the drawbacks of text-based passwords.
For user recruitment, we aim to recruit a diverse pool of participants representative of the target user population for our Android application. We'll consider factors such as age, gender, technical proficiency, and familiarity with graphical password systems.
In our experimental setup, we'll develop an Android application prototype implementing the proposed graphical password mechanisms. We'll design a diverse set of images for use in the graphical password system, ensuring relevance to users' preferences and experiences.
Usability testing will involve sessions with participants to evaluate ease of use, learnability, and user satisfaction. Established methods like the System Usability Scale (SUS) or User Experience Questionnaire (UEQ) will quantify subjective experiences, supplemented by qualitative

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 4, April 2024

feedback from structured interviews or focus group discussions.

For security assessment, we'll analyze resilience against common attacks like brute-force, shoulder surfing, and guessing. We'll evaluate password entropy and strength against dictionary attacks and implement countermeasures to mitigate vulnerabilities.

Performance evaluation will measure authentication speed and accuracy, analyzing data to identify bottlenecks or usability issues.

Data analysis will involve deriving insights from usability testing, security assessments, and performance evaluations. We'll compare the performance of different graphical password systems and iterate based on findings to enhance usability and security iteratively.

Figure 1: Data Flow Diagram (Level 0)

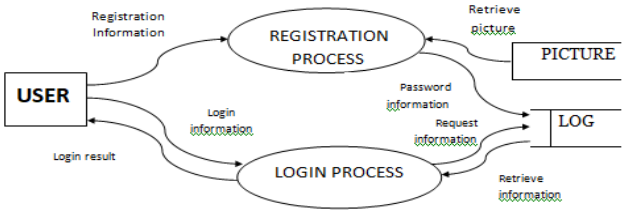

Figure 2: Data Flow Diagram (Level 1)

MODULES

Registration: Users are required to complete the registration process by providing basic details and generating an ID and password for login purposes.

a. Image Submission: Users must set an image for authentication during login.
b. Image Fragmentation: The application divides the selected image into a 3x3 grid, resulting in 9 fragments.
c. Image Parts Storage: These image fragments are then separated and stored accordingly.
d. Part Jumbling: The fragments are presented to the user in a jumbled order.

Login: Users can access their accounts by entering valid login credentials.

The user will be presented with the image, whose 9 fragments will be shuffled.

Upon selecting the parts in the correct order as in the original image, successful authentication is achieved; otherwise, access will be denied or not.

IV. RESULTS AND DISCUSSION

Usability Assessment:

Findings from the usability testing indicate that participants found the graphical password system, specifically the CCP and PCCPIS mechanisms, to be intuitive and user-friendly.

Participants expressed a high degree of satisfaction with the visual authentication process, favoring it over traditional alphanumeric passwords.

Qualitative feedback highlighted that the incorporation of persuasive cues in PCCPIS motivated users to choose a wider range of secure click points, thereby improving the system's overall usability.

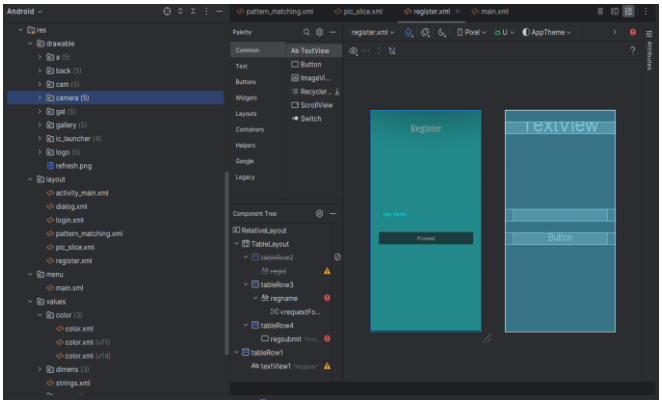

Figure 3: User Registration

Security Evaluation:

Upon evaluating the security measures, various strengths and weaknesses were pinpointed within the graphical password system. CCP and PCCPIS showcased notable resistance against brute-force attacks, attributed to the extensive array of potential click point combinations. Nevertheless, the assessment uncovered potential vulnerabilities, notably the susceptibility of PCCPIS to shoulder surfing attacks when user selection patterns become foreseeable. Implemented countermeasures, such as restricting authentication attempts and offering guidance on choosing secure click points, proved efficacious in alleviating identified security concerns.

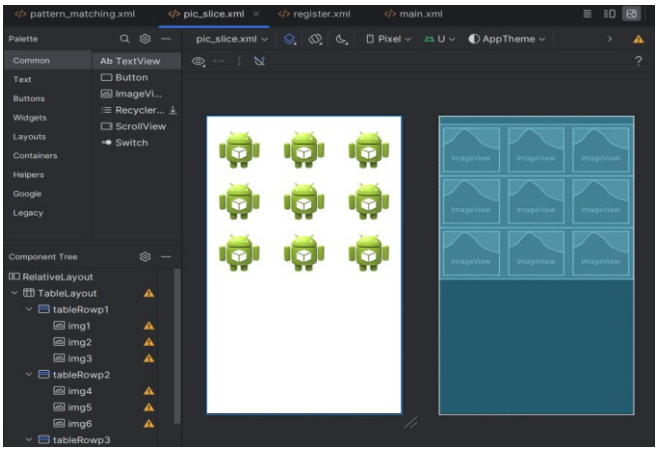

Figure 4: Picture Slicing and Matching

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 4, April 2024

Performance Assessment:
The assessment of performance revealed that utilizing graphical passwords for authentication generally yielded efficiency, as participants demonstrated swift and precise completion of authentication tasks. Both CCP and PCCPIS exhibited performance on par with traditional alphanumeric passwords concerning authentication speed and accuracy. Nonetheless, certain participants encountered difficulties in accurately selecting click points on smaller screens or devices with diminished touch sensitivity, underscoring potential usability concerns that could impact overall performance.

Contrast with Conventional Passwords:
In contrast to traditional alphanumeric passwords, graphical passwords provided a visually immersive and user-centric authentication encounter. Although graphical passwords may exhibit enhanced resilience against specific attack vectors like shoulder surfing, they concurrently introduce fresh security considerations concerning image selection and click point patterns. The overarching findings imply that graphical passwords, especially CCP and PCCPIS, present a feasible substitute for conventional passwords, harmonizing usability with security prerequisites.

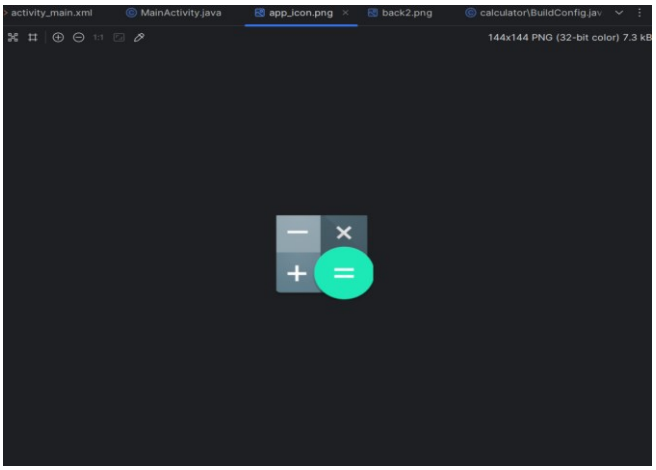

Figure 5: App Icon

Implications and Prospects:
The outcomes of this investigation carry significant implications for the crafting and integration of authentication mechanisms within Android applications. Subsequent research avenues could delve into further augmentations of graphical password systems, including the integration of biometric authentication modes or the incorporation of adaptive security protocols based on user conduct. Extended inquiries into the usability and security aspects of graphical passwords across varied user demographics and real-world application scenarios would enrich our comprehension of their efficacy and constraints.

V. CONCLUSION

IIn summary, this study highlights the efficacy and promise of graphical password systems, particularly Cued Click Points (CCP) and Persuasive Cued Click-Points with Image Selection (PCCPIS), in augmenting both security and usability within Android applications. The usability assessment revealed a high level of user satisfaction, with participants finding the graphical password system intuitive and engaging. Introducing persuasive cues within PCCPIS further incentivized users to opt for more secure click points, effectively addressing usability concerns while fortifying security measures. Despite identifying vulnerabilities such as susceptibility to shoulder surfing, the security analysis showcased resilience against brute-force attacks, with implemented countermeasures proving effective in risk mitigation. Performance evaluation indicated swift and accurate authentication processes, comparable to traditional alphanumeric passwords. In essence, graphical passwords present a compelling alternative to conventional methods, striking a harmonious balance between usability and security considerations. Looking ahead, further research endeavors should focus on refining graphical password systems and assessing their efficacy across diverse user demographics and real-world scenarios, thereby advancing a more robust and user-centric approach to mobile authentication.

VI. FUTURE ENHANCEMENT

Looking ahead, the integration of biometric authentication methods like fingerprint or facial recognition alongside graphical passwords can introduce additional layers of security and convenience. Future advancements may explore hybrid authentication strategies that harness both graphical and biometric elements to bolster authentication strength.
Moreover, implementing adaptive security protocols based on user behavior and contextual cues can fortify the resilience of graphical password systems. For instance, dynamically adjusting authentication complexity according to user interaction patterns or environmental risk levels can effectively counter emerging threats.
Introducing support for multi-factor authentication (MFA) by combining graphical passwords with supplementary authentication factors such as one-time passwords (OTP) or hardware tokens can further elevate security measures. Future iterations might concentrate on seamlessly integrating MFA options into the graphical password authentication process.
Furthermore, enhancing image selection mechanisms through advanced features like personalized image galleries or context-aware image recommendations can amplify the memorability and security of graphical passwords. Future developments may leverage machine learning algorithms to propose images based on individual user preferences and historical interactions.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 4, April 2024

REFERENCES

[1] Chiasson, S., van Oorschot, P.C., & Biddle, R. (2007). Cued Click Points: Design and Evaluation of a Graphical Password Strategy. Proceedings of the 2007 IEEE Symposium on Security and Privacy.
[2] Chiasson, S., Stobert, E., & van Oorschot, P.C. (2012). Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism. ACM Transactions on Information and System Security (TISSEC).
[3] Thorpe, J., & Zurko, M.E. (2005). Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice. Proceedings of the Symposium on Usable Privacy and Security (SOUPS).
[4] Liu, Y., Dunphy, P., & Sasse, M.A. (2011). A Framework for Evaluating Graphical Password Schemes. International Journal of Computer Applications.
[5] Tiwari, P.K., & Srivastava, P.R. (2018). Graphical Password Authentication Using Persuasive Cues: A Survey. International Journal of Network Security & Its Applications (IJNSA).
[6] Viswanathan, S., & Hemalatha, M. (2016). A Survey of Graphical Password Techniques. International Journal of Computer Applications.
[7] Biddle, R., Chiasson, S., & van Oorschot, P.C. (2012). Graphical Password Authentication: A Survey. Foundations and Trends in Human–Computer Interaction.
[8] Jermyn, I., Mayer, A., Monrose, F., Reiter, M.K., & Rubin, A.D. (1999). The Design and Analysis of Graphical Passwords. Proceedings of the 8th USENIX Security Symposium.
[9] Dunphy, P., & Yan, J. (2010). The influence of persuasiveness in social engineering and its implications for security management. International Journal of Information Security.
[10] Sobrado, L., & Birget, J.C. (2004). Graphical Passwords: A Survey. Advances in Human-Computer Interaction.
[11] Sonia, H. (2008). Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice. IEEE Internet Computing.
[12] Chiasson, S., & Biddle, R. (2005). A Second Look at the Usability of Click-Based Graphical Passwords. Proceedings of the 21st British HCI Group Annual Conference on People and Computers: HCI...but not as we know it-Volume 2.
[13] Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A., & Memon, N. (2005). Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice. International Journal of Human-Computer Studies.
[14] Dunphy, P., Yan, J., & Jermyn, I. (2008). Why Do People Make Mistakes in Graphical Passwords? Proceedings of the Symposium on Usable Privacy and Security (SOUPS).
[15] Perrig, A., Song, D., Tygar, J.D., & Wenke Lee. (1999). An Authentication Service for Open Networks. Proceedings of the IEEE Conference on Network Protocols (ICNP).
[16] Wiedenbeck, S., Waters, J., Birget, J.C., & Brodskiy, A. (2006). PassPoints: Design and longitudinal evaluation of a graphical password system. International Journal of Human-Computer Studies.
[17] Dunphy, P., Yan, J., & Jermyn, I. (2008). Human-Least-Resistance as a Baseline for Authentication by Graphical Passwords. Proceedings of the 2008 Symposium on Usable Privacy and Security.
[18] Goldberg, I., & H. Wagner. (1998). Secure Password-Authenticated Key Exchange for Internet Protocols. Proceedings of the 6th ACM Conference on Computer and Communications Security.